

Chapter 8

Privacy Preserving Federated Learning Frameworks for Secure, Scalable, and Citizen- Centric AI in Smart City Ecosystems


Anorgul Ashirova

Mamun University, Khiva, Uzbekistan

Nosir Khurramov


Termez University of Economics and Service, Termez, Uzbekistan

R. N. Ravikumar

 <http://orcid.org/0009-0009-3705-1681>

Marwadi University, Rajkot, India

S. Aarthi

 <http://orcid.org/0009-0006-9064-2091>

Marwadi University, Rajkot, India

S. Sindhuja

Kongu Engineering College, Erode, India

DOI: 10.4018/979-8-3373-4202-3.ch008

Copyright © 2026, IGI Global Scientific Publishing. Copying or distributing in print or electronic forms without written permission of IGI Global Scientific Publishing is prohibited. Use of this chapter to train generative artificial intelligence (AI) technologies is expressly prohibited. The publisher reserves all rights to license its use for generative AI training and machine learning model development.

ABSTRACT

Smart cities increasingly depend on data-driven intelligence to enhance healthcare, mobility, energy, and citizen services, yet centralized AI models raise concerns over privacy, security, and regulatory compliance. Federated Learning (FL) emerges as a privacy-preserving paradigm that trains models locally on IoT devices, smart meters, and mobile systems while sharing only model updates. This chapter explores FL's architecture, core components, and integration with enabling technologies such as Blockchain, Differential Privacy, and Edge AI. Real-world use cases, including Traffic Management, Healthcare Diagnostics, and Energy Optimization, demonstrate its transformative potential. Challenges like device heterogeneity, communication overhead, and data imbalance are critically analyzed, with solutions and future policy directions proposed to ensure ethical, secure, and sustainable adoption of FL in citizen-centric smart cities.

1. INTRODUCTION

The accelerated transformation of smart city also alters the way cities function by relying on data-driven systems, thereby making them the most efficient, sustainable, and healthy to the inhabitants. Nevertheless, this dependency on big data full of impersonal information to healthcare and energy consumption raises the privacy and security issue on a large scale. Conventional centralized machine learning models have higher chances of requiring that sensitive information be kept in a single database, which can become the source of a breach, intrusion, or violation of data protection regulations like GDPR (Jiang et al., 2020). Federated Learning (FL) has proven to resolve them as a consistent step in this direction, empowering the abilities of multi-participant intelligence without infringing on the privacy of one specific person. FL will also enable the models to train on the distributed devices and then secure aggregate rather than transmitting raw data to them. The plan does not only promote trust and resilience but as per the vision of smart cities that are people-centered. With complementary technologies such as a blockchain, differential privacy, and edge AI to FL, urban systems will have privacy-preserving, sustainable, and scalable intelligence.

1.1 The Need For Privacy In Urban AI Systems

By implementing artificial intelligence to enhance mobility, health care, energy management, and citizen services, cities have created challenges over privacy of urban AI systems and tools. Smart cities rely on the real-time information gathered

32 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/chapter/privacy-preserving-federated-learning-frameworks-for-secure-scalable-and-citizen-centric-ai-in-smart-city-ecosystems/407306

Related Content

The Role of Engineers and Their Tools in the Transport Sector after Paradigm Change: From Assumptions and Extrapolations to Science
Hermann Knoflacher (2017). *Engineering Tools and Solutions for Sustainable Transportation Planning* (pp. 1-29).

www.irma-international.org/chapter/the-role-of-engineers-and-their-tools-in-the-transport-sector-after-paradigm-change/177952

An Adaptive Elastic Net Method for Edge Linking of Images

Junyan Yi, Gang Yang, Xiaoxuan Ma and Xiaoyun Shen (2016). *Civil and Environmental Engineering: Concepts, Methodologies, Tools, and Applications* (pp. 921-930).

www.irma-international.org/chapter/an-adaptive-elastic-net-method-for-edge-linking-of-images/144531

Risk Analysis in the Process of Hydraulic Fracturing

Sonja Košak Kolinand Marin ikeš (2015). *Transportation Systems and Engineering: Concepts, Methodologies, Tools, and Applications* (pp. 1125-1140).

www.irma-international.org/chapter/risk-analysis-in-the-process-of-hydraulic-fracturing/128716

Project Maturity Analysis in Civil Construction

(2019). *Measuring Maturity in Complex Engineering Projects* (pp. 195-205).

www.irma-international.org/chapter/project-maturity-analysis-in-civil-construction/212399

Discrete Finite Element Method for Analysis of Masonry Structures

Iraj H. P. Mamaghani (2016). *Computational Modeling of Masonry Structures Using the Discrete Element Method* (pp. 393-415).

www.irma-international.org/chapter/discrete-finite-element-method-for-analysis-of-masonry-structures/155441